REMARKS

This communication is a full and timely response to the aforementioned Office Action dated September 30, 2008. By this communication, claims 1, 7 and 17 are amended, claims 25-27 are cancelled, and claims 28-31 are added. Claims 2-6, 8-12, 18-20 and 22-24 are not amended and remain in the application. Thus, claims 1-12, 17-20, 22-24 and 28-33 are pending in the application. Claims 1, 7, 17 and 31 are independent.

Reconsideration of the application and withdrawal of the rejections of the claims are respectfully requested in view of the foregoing amendments and the following remarks.

I. Rejections Under 35 U.S.C. § 103(a)

A. Claims 1, 4, 5, 7, 10, 12, 17, 20 and 22-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters (U.S. Patent Application Publication No. 2004/0088548, hereinafter "Smetters") in view of Benussi et al. (U.S. Patent Application Publication No. 2001/0044898, hereinafter "Benussi").

This rejection is believed to moot with respect to claim 25 in view of the cancellation of claim 25. This rejection is respectfully traversed with respect to claims 1, 4, 5, 7, 10, 12, 17, 20 and 22-24.

To establish a *prima facie* case of obviousness, the applied references must disclose or suggest all the claim limitations. See MPEP 2142; 706.02(j). If the applied references fail to disclose or suggest one or more of the features of a claimed invention, then the rejection is improper and must be withdrawn.

(1) Independent Claims 1, 7, 17 and 31

Claim 1 recites a communication system in which a device and a client communicate data with each other through a network. Claim 1 recites that the device comprises a first storage device which stores a root certificate including a public key paired with a private key and signed with the private key.

In addition, claim 1 recites that the device comprises a certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to sign the root certificate.

Claim 7 recites a communication method for a communication system in which a device and a client communicate date with each other through a network, wherein the device holds a root certificate including a public key paired with a private key and being signed with the private key.

In addition, the method of claim 7 includes the device creating, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being singed with the private key used to sign the root certificate when data is sent to the client.

Claim 17 recites a device to be used in a communication system in which the device and a client communicate with each other through a network, the device sends information to the client, and the client uses the information to communicate with the device. The device of claim 17 comprises a first storage device which stores a pair of a public key and a private key, and a second storage device which stores a root certificate signed with the private key.

In addition, the device of claim 17 comprises a certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to the sign the root certificate.

Claim 31 recites a computer-readable recording medium having a computer program recorded thereon that causes a computing device to perform operations of storing a pair of a public key and a private key, storing a root certificate signed with the private key, and sending information and the root certificate including the public key to the client, before a request for communication is requested by the client.

In addition, claim 31 recites that the computer program causes the computing device to perform an operation of creating, when the connection for communication is requested by the client, a second certificate designating the root certificate as a certificate authority at a higher level and being signed with the private key used to sign the root certificate.

Accordingly, independent claims 1, 7, 17 and 31 each recite that the device creates a second certificate, which designates the root certificate as a certificate authority at a higher level, where the second certificate is signed with the private key used to sign the root certificate, when a connection for communication is requested by the client.

Applicant respectfully submits that the applied references do not disclose or suggest the above-described features of independent claims 1, 7, 17 and 31 for at least the following reasons.

The Office asserted that the feature of a second certificate, which designates a root certificate as a certificate authority at a higher level, and which is signed with a private key is disclosed in Smetters. This assertion is contrary to the disclosure of Smetters. The actual disclosure of Smetters is summarized below, in view of the Office's unsupportable assertion that Smetters discloses that a second certificate is signed with a private key.

Smetters discloses a system 10 for creating a shared resource space 20 containing resources 22, 24 to be shared among a first device 12(1) and a second device 12(2) (see Figures 1 and 3). The first device 12(1), which has access to the resources 22, 24, generates a root key pair to be used for authentication and encryption when providing the device 12(2) with access to the shared space 20 (see paragraph [0025], step 100 in Figure 2, and step 120 in Figure 4). In order to share access to the space 20, the first device 12(1) then "generates a root certificate 30 for the new space 20, and digitally signs the [root] certificate 30" (see paragraph [0025], step 100 in Figure 2, and step 130 in Figure 4) (emphasis added).

Based on the disclosure in paragraph [0025], which clearly refers to the root certificate 30, not a second certificate, the Office asserted on page 3 of the Office Action that Smetters discloses that a second certificate 40 generated by the first device 12(1) is somehow signed with a private key. In particular, the Office asserted that, based on the above-quoted paragraph [0025] of Smetters, "[i]t is well known in the art that digital certificates are signed with a certificate authority's private key. This is how certificates operate. For example, this is [shown] in Smetters paragraph 25." The Office further asserted that "signing certificates with a private key is discussed in the new [applied] references...as well." (see page 3 of Office Action)

The Office is erroneously interpreting disclosures of a root certificate being signed with a private key for disclosures where a second certificate is signed with a private key. None of the applied references disclose or suggest that a second certificate, which designates the root certificate as a certificate authority at a higher level, is signed with the private key used to sign the root certificate.

Applicant respectfully submits that the Office is misinterpreting the recitation of the second certificate as recited in claims 1, 7, 17 and 31. As is evident from the-above-quoted paragraph [0025], Smetters discloses that the root certificate is digitally signed by the first device 12(1). Smetters, however, does not disclose or suggest that a second certificate 40 generated by the first device 12(1) is signed with the private key used to sign the root certificate 30. On the contrary, Smetters discloses an opposite technique in which the second certificate 40 is signed with a public key that is (i) generated by the first device 12(1), or (ii) generated by the second device 12(2) and transmitted to the first device 12(1) by the second device 12(2). The actual disclosure of Smetters is summarized below to illustrate this distinction between Smetters and the claimed invention.

Smetters discloses that after the first device 12(1) has generated the root certificate 30, the first device 12(1) then transmits range-limited signals to the second device 12(2) to establish a secure communication channel between each other (see paragraph [0028], step 200 in Figure 2). Paragraph [0028] of Smetters also discloses that the second device 12(2) may initially send the range-limited signals to initiate the establishment of a secure communication channel with the first device 12(1). Smetters discloses that the range-limited signal transmitted from the first device 12(1) includes a public key to secure the communication channel between the first and second devices 12(1), 12(2) (see paragraph [0029]). Once a secure communication channel between the first device 12(1) and second device 12(2) has been established, Smetters discloses that the first device 12(1) then sends an invitation message to the second device 12(2) that invites the second device 12(2) to accept access to the shared space 20 (see paragraph [0030], and step 300 in Figure 2).

Smetters discloses that the second device 12(2) then decides whether to use a particular public key (i.e., the public key included in the range-limited signal from the first device 12(1) or a public key generated by the second device 12(2)) to communicate with the first device 12(1) (see paragraph [0032] and step 510 in Figure 6). If the second device 12(2) decides to use a particular public key instead of the public key included in the range-limited signal from the first device 12(1), the second device 12(2) transmits the desired public key to the first device 12(1) (see paragraph [0032] and step 520 in Figure 6). On the other hand, if the second device 12(2) decides to use the public key generated by the first device 12(1) and included in the range-limited signal, the first device 12(1) generates a pair of a public key and a private key, and sends the private key of the generated key pair to the second device 12(2) (see paragraph [0033], and steps 530 and 540 in Figure 6). If the second device 12(2) desires to use the public key generated by the first device 12(1), the first device 12(1) must therefore send the corresponding private key to the second device 12(2), or else the second device 12(2) could not decrypt a communication that was encrypted with the public key generated by the first device 12(1). On the other hand, if the second device 12(2) decides to use a particular public key for encryption instead of the public key generated by the first device 12(1), it is not necessary for the first device 12(1) to transmit the corresponding private key to the second device 12(2), because the corresponding private key 12(2) is already in the possession of the second device 12(2).

Then, to provide the second device 12(2) with access to the shared space 20, Smetters discloses that the first device 12(1) creates a second certificate 40 using either the public key sent from the second device 12(2) or the public key of the key pair generated by the first device 12(1) (see paragraph [0034], step 500 in Figure 2, and step 550 in Figure 6). The second certificate 40 designates the second device 12(2) as a member of the shared space 20 (see paragraphs [0031] and [0034], step 500 in Figure 2, and step 550 in Figure 6). Smetters discloses that the first device 12(1) sends both the root certificate 30 and the second certificate 40 to the second device 12(2) at the same time as a certificate chain (see paragraph [0035]).

Paragraph [0031] of Smetters discloses that "the second laptop certificate 40 is the same as the root certificate, except as described herein." Based on this statement, the Office asserted that the second certificate 40 is signed with a private key. Applicant respectfully submits that the Office has neglected the phrase "except as described herein," and instead focused solely on the former phrase in the above-quoted sentence in paragraph [0031] to arrive at its erroneous interpretation that the second certificate 40 of Smetters is signed with a private key. Applicant respectfully submits that this assertion is contradictory to the disclosure of Smetters.

The Office appears to presume that because the second certificate 40 is "the same as the root certificate [30]" (see paragraph [0031]), the second certificate 40 must therefore be signed with a private key. However, Smetters discloses an opposite configuration, in which the second certificate 40 is signed using either (1) the public key sent from the second device 12(2) or (2) the public key of the key pair generated by the first device 12(1) (see paragraph [0034], step 500 in Figure 2, and step 550 in Figure 6). Signing the second certificate 40 with a private key is contrary to the disclosure of Smetters.

As noted above, Smetters discloses two techniques for generating and signing the second certificate: (1) the second device 12(2) transmits a particular public key to the first device 12(1) for signing the second certificate 40, or (2) the first device 12(1) generates the public key and signs the second certificate 40 with the generated public key. The first technique (1) is illustrated in Figure 6 with respect to step 520. In this technique, <u>the second device 12(2) retains the private key</u> corresponding to the public key transmitted to the first device 12(1), because the first device 12(1) signs the second certificate 40 with the public key and the second device 12(2) must therefore possess the corresponding private key in order to decrypt the second certificate 40. In public-private key cryptography, encrypted data can only be decrypted by using one key of a key pair, when the other key of the key pair was used to encrypt the key pair. Therefore, in view of the disclosure of Smetters that the second device 12(2) sends the public key to be used in signing the second certificate 40 to the first device 12(1), the second device 12(2) must retain possession of the corresponding private key in order to decrypt the second certificate 40 sent from the first device 12(1).

Furthermore, Applicant respectfully submits that it is not possible for the first device 12(1) to sign the second certificate 40 with a private key corresponding to the public key transmitted from the second device 12(2), because Smetters does not disclose or suggest that the second device 12(2) transmits the private key corresponding to the public key that was transmitted from the second device 12(2). Moreover, such an interpretation would be contradictory to the principles of public-private key cryptography.

Therefore, according to the first technique (1) in which the second device 12(2) transmits a public key to the first device 12(1) and the first device 12(1) signs the second certificate 40 with the public key received from the second device 12(2), the first device 12(1) does not sign the second certificate 40 with a private key corresponding to the public key transmitted from the second device 12(2).

Furthermore, the first device 12(1) does not sign the second certificate 40 with the private key used to sign the root certificate 30. Such a construction would not be possible according to the first technique (1) of Smetters, because the root certificate 30 is generated by the first device 12(1) after the first device 12(1) has generated a root key pair (see paragraph [0025]), and the second certificate 40 is generated by the first device 12(1) using the public key transmitted from the second device 12(2). A public or private key of one root key pair does not correspond to a public or private key of another root key pair. Accordingly, it would not be possible according to the first technique (1) of Smetters for the first device 12(1) to sign the second certificate 40 with the same private key used to sign the root certificate 30, because different key pairs are used for generating the root certificate 30 and the second certificate 40.

The second technique (2) of Smetters is illustrated in Figure 6 with respect to steps 530 and 540. In this technique, the first device 12(1) generates a public and private key pair (step 530), and sends the private key corresponding to the public key pair to the second device 12(2) (see paragraph [0033]). The first device 12(1) must send the private key corresponding to the public key that is used to sign the second certificate 40, because the second device 12(2) would not be able to decrypt the second certificate 40 unless it was provided with the private key. The disclosure in paragraph [0033] further emphasizes that the first device 12(1) does not sign the second certificate 40 with the private key corresponding to the public key, because sending the private key of the newly generated key pair to the second device 12(2) would not, in any way, permit the second device 12(2) to decrypt the second certificate 40, if the second certificate 40 was hypothetically signed with the private key of the newly generated key pair. If the second certificate 40 was hypothetically signed with the private key of the newly generated key pair, then the first device 12(1) would need to send the public key of the newly generated key pair, so that the second device 12(2) could decrypt the second certificate 40. However, Smetters discloses the opposite technique in which the first device 12(1) transmits the private key to the second device 12(1), because the second certificate 40 is signed with the public key of the key pair that is newly generated by the first device 12(1).

Therefore, according to the second technique (2) of Smetters in which the first device 12(1) generates a new key pair and transmits the private key of the newly generated key pair to the second device 12(2), Smetters does not disclose or suggest that the second certificate 40 is signed with a private key.

Furthermore, the first device 12(1) does not sign the second certificate 40 with the private key used to sign the root certificate 30. Such a construction is contradictory to the disclosure of Smetters. In particular, Smetters discloses that when the second device 12(2) elects to have the first device 12(1) use a public key generated by the first device 12(1) to generate the second certificate 40, the first device 12(1) generates a new key pair (see paragraph [0033, and step 530 in Figure 6]). The new key pair generated by the first device 12(1) to generate the second certificate 40 in step 530 of Figure 6 (corresponding to step 500 in Figure 2) is different from the key pair generated by the first device 12(1) to generate the root certificate 30 in step 120 of Figure 4 (corresponding to step 100 in Figure 2), because these key pairs are generated at different stages within the resource management process of Figure 2 and therefore are different key pairs. Consequently, Smetters does not disclose or suggest that the first device 12(1) signs the second certificate 40 with the private key used to sign the root certificate 30.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that Smetters does not disclose or suggest that the second certificate 40 (or any other subordinate member certificate) is signed with the private key used to sign the root certificate 30.

Therefore, Smetters does not disclose or suggest that the device creates a second certificate, which designates the root certificate as a certificate authority at a higher level, where the second certificate is signed with the private key used to sign the root certificate, when a connection for communication is requested by the client, as recited in claims 1, 7, 17 and 31.

Benussi also does not disclose or suggest these features of claims 1, 7, 17 and 31. On the contrary, Benussi discloses that a root certificate ("Root CA") of a CSS (communication service system) 20 is signed with a private key of the CSS 20, and the root certificate of CSS 20 is pre-installed in the CB (connectivity box) 11 for the initial configuration of the CB 11 (see paragraph [0214], lines 24-30 and 51-55, and Figure 1).

However, similar to Smetters, Benussi does not disclose or suggest that a second certificate, which designates the Root CA of the CSS 20 as a certificate authority at a higher level, is signed with the private key of the CSS 20 used to sign the Root CA.

Therefore, neither Smetters nor Benussi disclose or suggest that the device creates a second certificate, which designates the root certificate as a certificate authority at a higher level, where the second certificate is signed with the private key used to sign the root certificate, when a connection for communication is requested by the client, as recited in claims 1, 7, 17 and 31.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that Smetters and Benussi, either individually or in combination, do not disclose or suggest all the recited features of claims 1, 7, 17 and 31.

Therefore, Applicant respectfully submits that claims 1, 7, 17 and 31 are patentable over Smetters and Benussi, since Smetters and Benussi, either individually or in combination, fail to disclose or suggest all the recited features of claims 1, 7, 17 and 31.

Furthermore, Applicant respectfully submits that the Office's proposed combination of Smetters and Benussi in an attempt to arrive at the subject matter of the claimed invention is not supportable.

It is well-settled that if a modification of an applied reference would change the principle of operation of the reference being modified, then there is no reason, suggestion or motivation to modify the reference in that manner. See In re Ratti, 123 USPQ 349 (CCPA 1959); MPEP 2143.01.VI.

However, in the present instance, the Office is proposing to change the principle of operation of Smetters in an attempt to arrive at the subject matter of the claimed invention. In particular, a major emphasis of Smetters is for the first device 12(1) to transmit both the root certificate 30 and the second certificate 40 at the same time, and the second device 12(2) stores the simultaneously received root and second certificates 30 and 40 together as a "certificate chain" (see paragraph [0305] and step 600 in Figure 2). As disclosed in paragraph [0305], the second device 12(2) uses the certificate chain to prove to other members of the shared space 20 that the second device 12(2) is authorized to access the shared space 20.

In contrast to the well-settled provisions of the impermissibility of changing the principle of operation of an applied reference, the Office proposed, on page 4 of the Office Action, that it would have been obvious to modify Smetters "to have stored the root certificate earlier." However, such a modification changes a principle of operation of Smetters, and therefore is not supportable.

Accordingly, in addition to Smetters and Benussi failing to disclose or suggest all the recited features of claims 1, 7, 17 and 31, Applicant respectfully submits that the proposed combination of Smetters and Benussi is not supportable.

(2) Dependent Claims

Dependent claims 4, 5, 10, 12, 20, 22-24, 28-30, 32 and 33 recite further distinguishing features over Smetters and Benussi.

For example, claim 10 recites that, in the method of claim 7, when the client installs the root certificate, the installation is performed after the root certificate is confirmed by a user. In an attempt to arrive at the features of claim 10, the Office referred to paragraph [0031] of Smetters, which discloses that the operator of the second device 12(2) decides whether to respond to the invitation from the first device 12(1) to gain access to the shared space 20. This does not amount to the features recited in claim 10, because Smetters does not disclose, suggest or contemplate that the operator of the second device 12(2) confirms the root certificate 30 prior to its installation. On the contrary, paragraph [0031] of Smetters merely discloses that the operator 12(2) decides whether he or she wants to gain access to the shared space 20, in response to the invitation message transmitted from the first device 12(1).

Claim 20 recites that the root certificate stored in the first storage device is stored in the second storage device prior to the transmission of the second certificate from the communication device. Claim 23 recites that, in the method of claim 7, the device sends the second certificate to the client after the root certificate is installed in the client.

As discussed above, a major emphasis of Smetters is for the first device 12(1) to send both the root certificate 30 and the second certificate 40 to the second device 12(2) at the same time, and for the second device 12(2) to store the received certificate chain so as to be able to prove that it has access to the shared resource space. Accordingly, Smetters discloses an opposite technique to the features of claims 20 and 23.

In an attempt to cure the deficiencies of Smetters, the Office has improperly changed a principle of operation of Smetters by applying Benussi. The improper combination of Smetters and Benussi is contrary to well-settled provisions, and therefore, Applicant respectfully submits that the combination of Smetters and Benussi to arrive at the features of claims 20 and 23 is not supportable.

Claim 22 recites that the verifier of the client is operable to verify the signature of the second certificate by decrypting the public key of the root certificate stored in the second storage device to obtain a first hash value, calculating a second hash value of the second certificate received from the device, and comparing the first and second hash values to determine if they are equal to each other.

The Office asserted that the features recited in claim 22 are disclosed in paragraphs [0041] and [0042] of Smetters. This assertion is not supportable. Paragraphs [0041] and [0042] of Smetters do not disclose or suggest the calculation of the first and second hash values and the subsequent comparison of the first and second hash values, as recited in claim 22. Paragraphs [0041] and [0042] do not disclose or suggest the generation of hash values from either the root certificate 30 or the second certificate 40.

Claims 28 and 29 recite that the client stores the public key of the installed root certificate, prior to the client requesting the connection for communication to the device, and that the client verifies the signature of the second certificate received from the device by decrypting the second certificate with the public key of the root certificate stored in the client.

Smetters and Benussi do not disclose or suggest the features of claims 28 and 29. In particular, as discussed above, Smetters discloses that the second device 12(1) decrypts the second certificate 40 by using the private key that is either sent from the first device 12(1) (when the first device 12(1) generates a new key pair for the second certificate 40) or is already installed in the second device 12(2) (when the second device 12(2) transmits the public key for creation of the second certificate 40). Accordingly, Smetters does not disclose or suggest that the second device 12(2) verifies the signature of the second certificate 40 by decrypting the second certificate 40 with the public key of the root certificate 30.

Furthermore, Benussi does not disclose or suggest any second certificate corresponding to the claimed invention. Therefore, Applicant respectfully submits that claims 28 and 29 recite further distinguishing features over the applied references.

For at least the foregoing reasons, Applicant respectfully submits that Smetters and Benussi, either individually or in combination, do not disclose or suggest the features of dependent claims 10, 20, 22, 23, 28 and 29, in addition to failing to disclose or suggest all the recited features of claims 1, 7, 17 and 31.

Therefore, in addition to the patentability of claims 1, 7, 17 and 31 demonstrated above, Applicant respectfully submits that claims 10, 20, 22, 23, 28 and 29 recite further distinguishing features over Smetters and Benussi.

B. Dependent claims 2, 3, 6, 8, 9, 11, 18, 19, 26 and 27 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Smetters in view of Benussi and further in view of one or more of Frailong et al. (U.S. Patent No. 6,012,100, hereinafter "Frailong'), Debry (U.S. Patent No. 6,918,042, hereinafter "Debry"), Slick (U.S. Patent Application Publication No. 2004/0109568, hereinafter "Slick"), and Vogel et al. (U.S. Patent No. 6,816,900, hereinafter "Vogel").

As demonstrated above, Smetters and Benussi each do not disclose or suggest a device that creates a second certificate, which designates the root certificate as a certificate authority at a higher level, where the second certificate is signed with the private key used to sign the root certificate, when a connection for communication is requested by the client, as recited in claims 1, 7, 17 and 31.

Similarly, Frailong, Debry, Slick and Vogel also each fail to disclose or suggest these features of claims 1, 7, 17 and 31. Therefore, Frailong, Debry, Slick and Vogel cannot cure the deficiencies of Smetters and Benussi for failing to disclose or suggest all the recited features of claims 1, 7, 17 and 31, since the applied references, either individually or in combination, do not disclose or suggest all the recited features of claims 1, 7, 17 and 31.

Therefore, no obvious combination of Smetters, Benussi, Frailong, Debry, Slick and Vogel would arrive at the subject matter of the claimed invention, since the applied references, either individually or in combination, fail to disclose or suggest all the recited features of at least claims 1, 7, 17 and 31.

Accordingly, for at least the foregoing reasons, Applicant respectfully submits that claims 1, 7, 17 and 31, as well as claims 2-6, 8-12, 18-20, 22-24, 28-30, 32 and 33 which depend therefrom, are patentable over the applied references.

The foregoing explanation of the patentability of independent claims 1, 7, 17 and 31 is sufficiently clear such that it is believed to be unnecessary to separately demonstrate the patentability of the dependent claims not specifically addressed above at this time. However, Applicant reserves the right to do should it become appropriate. Furthermore, Applicant does not acquiesce to any of the Office's assertions not specifically addressed above. Applicant reserves the right to address any of the Office's assertions not specifically addressed above should it become appropriate.

II. Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. Accordingly, a favorable examination and consideration of the instant application are respectfully requested.

If, after reviewing this Amendment, the Examiner believes there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: December 29, 2008

By: /Jonathan R. Bowser/
Jonathan R. Bowser
Registration No. 54574

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620